RETEX ON A FEW CALLS
HERVÉ DEBAR

Institut Mines-Télécom

SU-INFRA01-2018-2019-2020

2

Prévention, détection, réponse et atténuation des menaces physiques et des cyber menaces sur les infrastructures critiques

- ## Challenge
  - Cyber-physical infrastructures:
    - *difficult to get access to in projects*
    - *difficult to create realistic attacks*
  - Automation:
    - *reluctance to access real systems and automate actions*
- ## Scope
  - 2020 should focus on interependencies
  - Assess in detail all aspects of interdependent physical and cyber threats and incidents
    - *Makes sense: ubiquitous digital control*
  - demonstrate the accuracy of their risk assessment approach using specific examples and scenarios of real life and by comparing the results with other risk assessment methodologies
    - *Requires access to real incident data ?*
    - *Privacy issues*
  - develop improved real-time, evidence-based security management of physical and cyber threats, taking account of the ageing of existing infrastructure
    - *Not easy for « IT guys »*
    - *Access usually difficult*
  - provide scenarios and recommendations for policy planning
    - *From EUNITY: this should be really short and liaise with the PO in order for the recommendations to have impact. If it works it is really good*

Institut Mines-Télécom

Challenge

- forecast, monitor and update the security of their ICT systems
  - ► *Missing: information models, but they are hard to get up and running*
  - ► *CTI is a strong topic in pilot projects*
- relying as appropriate on Artificial Intelligence and automation
- Detection and mitigation of cyberthreats for algorithms
  - ► *Linked to explainable AI*
  - ► *Strong topic in pilot projects*

Scope

- Sous topic a): Gouvernance dynamique, gestion des risques et conformité
  - ► *Mention of cyber-ranges, actively developed in the pilot projects*
  - ► *Many activities are related to SIEM, and there have been several funded projects in FP7 and H2020*
  - ► *Significant SHS (economic, legal, ethical) component*
- Sous-topic b): Partage et analyse des informations sur les cybermenaces
  - ► *CTI: strong in pilot projects, but difficult to organize*
  - ► *Include CERTs in operations, but this is a different community (e.g. CEF Telecom call). Maturity levels are significantly different*
  - ► *Existing models: MISP platform*

Institut Mines-Télécom

- **End users et expérimentations**
  - Cas d'usages « réalistes »
  - En « contradiction » avec certains aspects des projets, e.g. Open Data Pilot et Data Management Plan
- **Relation avec ce qui a déjà été financé**
  - Réutilisation des résultats produits dans des projets précédents
- **Focus sur des résultats tangibles**
  - Démonstrations
  - Nombre important de end-users
- **Taille croissante des consortiums gagnants**
- **Possibilité de développer les résultats dans d'autres frameworks européens**

Institut Mines-Télécom